# Introduction to the Minitrack on Insider Threats to Governments and Organizations

Matt Bishop
University of California at Davis
mabishop@ucdavis.edu

Jay Kesan
University of Illinois at Urbana-Champaign
kesan@illinois.edu

Jason Clark
Software Engineering Institute, Carnegie Mellon University
jwclark@cert.org

The insider problem is one of the most important problems in computer security, and indeed in all aspects of real-world security. Insiders have compromised many key societal systems and processes in domains such as government, finance, anThe insider problem is one of the most important problems in computer security, and indeed, in all aspects of real-world security. Insiders have compromised many key societal systems and processes in domains such as government, finance, and even science. Many reports of insider attacks describe people trusted with access to sensitive information abusing that access to damage that information, compromise the privacy of that information, and collaborate with others (sometimes other insiders) to cause various kinds of failures, losses and serious harm. Indeed, the insider problem is also pernicious in the non-computer world; as the ancient Roman satirist Juvenal said, "Who will guard the guards themselves?" Any approaches therefore must have not only a technical aspect, but also a non-technical (social, political, legal, cultural, and so forth) approach. Insider attacks may be accidental or arise from conflicting policies that confuse the putative attacker. These unintentional insider attacks are as dangerous as deliberate insider attacks, but must be handled differently due to the lack of maliciousness. Understanding how to cope with unintentional insider attacks effectively is also a complex, difficult problem.

URI: http://hdl.handle.net/10125/50193
ISBN: 978-0-9981331-1-9